1.0 Introduction

Vulnerabilities may be identified on campus servers or applications that for legitimate reasons may not be patched or removed. The most common reasons are that a vendor will not support moving to secure operating systems or middleware applications, or due to other hardware or software dependencies.

2.0 Purpose

The purpose of this procedure is to outline the process for requesting and approving server, application, or middleware vulnerability exceptions.

3.0 Scope

This procedure applies to all devices, applications and web applications connected to or hosted by the Sacramento State network, including but not limited to, servers, workstations, network appliances, cameras, printers, and multi-function copiers

4.0 Procedure

4.1 Initiating exception requests

Departments that wish to request vulnerability exception requests should create a ticket in Servicenow using catalog item?? The ticket should include a list of all QIDs, and be assigned to the ISO Team for review.

• Under Policy/Standard Requiring Exception, list the name and/or IP address/URL/QID that you are requesting the exception for.

• Under Business/Technical Justification, enter a justification(s).

• Under Compensating Controls, list compensating controls which may mitigate the risk identified. A compensating control is security mitigation such as additional restricted user access, network segmentation, or monitoring which would mitigate a specific exploit or system weakness.

4.2 Exception Processing (ISO)

4.3 Generate Risk Report

ISO will develop a risk report which includes information about the server, server/application name, department, department admin, location, purpose, Level 1 data presence, authentication status, hosted web applications, operating system, and any firewall exceptions; all vulnerabilities with QIDs and titles; any approved border firewall exceptions; and results from an Identity Finder scan. ISo Completes Security Exception Form.

ISO will complete a Security Exception form based on the information supplied by the request.

4.4 Required Vulnerability Management

4.5 Vulnerability Exception Review and Approval

The Information Security Officer or Chief Information Officer will review vulnerability exceptions to identify risk and evaluate proposed mitigations.

4.6 Vulnerability Exception Review

The completed exception justification form will be routed to the department for administrative review and approval. Completed form should be returned to ISO.

4.7 Vulnerability Reporting for Exceptions

Approved security exceptions will be added to the next monthly report. Servers with approved exceptions will be highlighted.

4.8 Exception Review

All vulnerability exceptions must be reviewed and risk accepted every 90 days

4.9 Server versus Application Exceptions, QID Exceptions

The ISO will maintain a list sorting QIDs based on Operating System or application. The ISO will maintain a list of QIDs tied to systems which have been granted exceptions. This list must be reviewed monthly.

5.0 Definitions

ISO – Information Security Office

QID- The Qualys ID number assigned to a vulnerability

6.0 Documentation History

Review/Approval History

Date	Audience	Action	Version